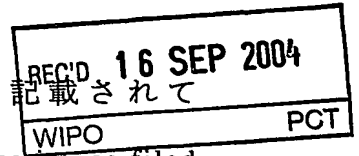


日 本 国 特 許 庁  
JAPAN PATENT OFFICE

26.07.2004

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

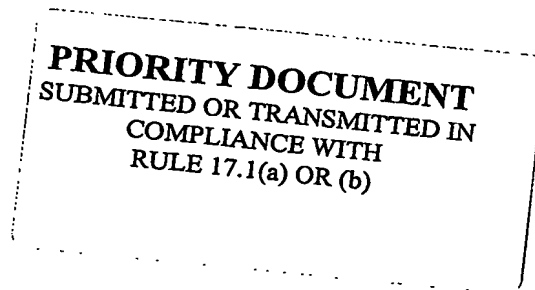
This is to certify that the annexed is a true copy of the following application as filed  
with this Office.



出 願 年 月 日  
Date of Application: 2 0 0 3 年 1 0 月 3 日

出 願 番 号  
Application Number: 特 願 2 0 0 3 - 3 4 6 2 1 7  
[ST. 10/C]: [ J P 2 0 0 3 - 3 4 6 2 1 7 ]

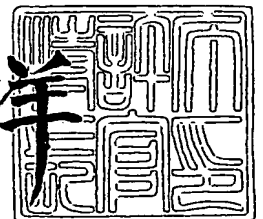
出 願 人  
Applicant(s): シャープ株式会社



2 0 0 4 年 9 月 3 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川 洋



【書類名】 特許願  
【整理番号】 03J03619  
【提出日】 平成15年10月 3日  
【あて先】 特許庁長官殿  
【国際特許分類】 G11B 11/00  
G06F 9/06

【発明者】  
【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内  
【氏名】 木付 英士

【発明者】  
【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内  
【氏名】 大泉 勝志

【発明者】  
【住所又は居所】 大阪府大阪市阿倍野区長池町 2 2 番 2 2 号 シャープ株式会社内  
【氏名】 木山 次郎

【特許出願人】  
【識別番号】 000005049  
【氏名又は名称】 シャープ株式会社  
【代表者】 町田 勝彦

【代理人】  
【識別番号】 100079843  
【弁理士】  
【氏名又は名称】 高野 明近

【選任した代理人】  
【識別番号】 100112313  
【弁理士】  
【氏名又は名称】 岩野 進

【手数料の表示】  
【予納台帳番号】 014465  
【納付金額】 21,000円

【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 0208586

**【書類名】 特許請求の範囲****【請求項 1】**

A V データ又はアプリケーションプログラム／データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置において、前記処理手段は、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴とする記録再生装置。

**【請求項 2】**

請求項 1 に記載の記録再生装置において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを有し、前記処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールするインストール処理手段を有することを特徴とする記録再生装置。

**【請求項 3】**

請求項 2 に記載の記録再生装置において、前記インストール処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴とする記録再生装置。

**【請求項 4】**

請求項 2 又は 3 に記載の記録再生装置において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記特定領域への書き込み処理を実行できないようにしたことを特徴とする記録再生装置。

**【請求項 5】**

請求項 1 又は 2 に記載の記録再生装置において、コンテンツの実行領域であるメモリを有し、前記処理手段は、前記記録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードするロード処理手段を有することを特徴とする記録再生装置。

**【請求項 6】**

請求項 5 に記載の記録再生装置において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴とする記録再生装置。

**【請求項 7】**

請求項 1 乃至 6 のいずれか 1 に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とする記録再生装置。

**【請求項 8】**

請求項 1 乃至 7 のいずれか 1 に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とする記録再生装置。

**【請求項 9】**

請求項 1 乃至 8 のいずれか 1 に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とする記録再生装置。

**【請求項 10】**

請求項 1 乃至 9 のいずれか 1 に記載の記録再生装置において、前記記録手段は、コンテ

ンツの再生又は実行に必要なプログラム及びデータを1つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段は、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段は、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴とする記録再生装置。

【請求項11】

請求項1乃至10のいずれか1に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該再生又は実行中のコンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴とする記録再生装置。

【請求項12】

請求項1乃至11のいずれか1に記載の記録再生装置において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴とする記録再生装置。

【請求項13】

請求項12に記載の記録再生装置において、前記コンテンツの信頼度を、プログラムの記述言語、前記読込手段によって読み込んだコンテンツの読込元となる記録媒体、前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか1又は複数に基づいて設定したことを特徴とする記録再生装置。

【請求項14】

AVデータ又はアプリケーションプログラム／データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置を用いてコンテンツの構成ファイルへアクセスするためのファイルアクセス方法において、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴とするファイルアクセス方法。

【請求項15】

請求項14に記載のファイルアクセス方法において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを前記記録再生装置が備え、前記処理手段が備えるインストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールすることを特徴とするファイルアクセス方法。

【請求項16】

請求項15に記載のファイルアクセス方法において、前記インストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴とするファイルアクセス方法。

【請求項17】

請求項15又は16に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記記録手段の特定領域への書き込み処理を実行できないようにしたことを特徴とするファイルアクセス方法。

【請求項18】

請求項14又は15に記載のファイルアクセス方法において、コンテンツの実行領域であるメモリを前記記録再生装置が備え、前記処理手段が備えるロード処理手段が、前記記録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードすることを特徴とするファイルアクセス方法。

**【請求項 19】**

請求項 18 に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴とするファイルアクセス方法。

**【請求項 20】**

請求項 14 乃至 19 のいずれか 1 に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とするファイルアクセス方法。

**【請求項 21】**

請求項 14 乃至 20 のいずれか 1 に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とするファイルアクセス方法。

**【請求項 22】**

請求項 14 乃至 21 のいずれか 1 に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴とするファイルアクセス方法。

**【請求項 23】**

請求項 14 乃至 22 のいずれか 1 に記載のファイルアクセス方法において、前記記録手段は、コンテンツの再生又は実行に必要なプログラム及びデータを 1 つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段が、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段が、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴とするファイルアクセス方法。

**【請求項 24】**

請求項 14 乃至 23 のいずれか 1 に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴とするファイルアクセス方法。

**【請求項 25】**

請求項 14 乃至 24 のいずれか 1 に記載のファイルアクセス方法において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴とするファイルアクセス方法。

**【請求項 26】**

請求項 25 に記載のファイルアクセス方法において、前記コンテンツの信頼度を、プログラムの記述言語、前記読込手段によって読み込んだコンテンツの読込元となる記録媒体、前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか 1 又は複数に基づいて設定したことを特徴とするファイルアクセス方法。

【書類名】明細書

【発明の名称】記録再生装置及びファイルアクセス方法

【技術分野】

【0001】

本発明は、記録再生装置及びファイルアクセス方法、より詳細には、A Vデータやアプリケーションプログラムもしくはアプリケーションプログラムが使用するデータを含むコンテンツを記録、再生、実行可能な記録再生装置及びそのファイルアクセス方法に関する。

【背景技術】

【0002】

D V DプレーヤやD V Dレコーダ等の普及により、H D Dを内蔵した複合型D V Dレコーダなどが市場に現れはじめた。また、例えばJ a v a (R) 言語などの普及により携帯電話などの端末機にもアプリケーションの実行環境が普及し始めた。しかしながら、任意のアプリケーションが実行可能である場合、あらゆる情報へのアクセスを認めることは危険である。そのため、特定のアプリケーション（例えば、i アプリ (R) など）では、信頼できるアプリケーションに限り、携帯電話の保持する電話帳などの各種情報へのアクセスを許可している。

【0003】

通常、端末にダウンロードされたアプリケーションは、不正な動作を行う可能性があるため、アプリケーションの動作は厳格に制限され、アプリケーションはローカルリソースを用いることができないようになっている。

これに対し、認証モジュールの耐タンパ領域に保持されるアプリケーションの認証情報を用いて、端末にダウンロードされたアプリケーションの認証を行い出所の確認や改ざんが行われていないかどうか確認し、認証されたアプリケーションのみ端末のローカルリソースの利用を許可するようにしたものが開示されている（例えば、特許文献1参照）。

【特許文献1】特開2003-223235号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

ここで、アプリケーションを実行可能な端末装置にローカルストレージを導入し、そのローカルストレージにおいて任意のアプリケーションを実行した場合、そのアプリケーションがコンテンツの作成者の意図に反してコピーや改ざんなどを行う可能性があるため、これに対する対策が必要となる。

また、アプリケーションの入手経路が複数ある場合、信頼性が低く悪意を持ったアプリケーションが実行される可能性がある。そこで、そのアプリケーションの信頼性に応じて各種情報に対するアクセス制限を行う必要がある。

【0005】

本発明は、上述のごとき実情に鑑みてなされたものであり、A Vデータ又はアプリケーションプログラム／データを含むコンテンツを記録した外部記録媒体やサーバ装置にアクセスして該コンテンツをローカルストレージに記録すると共に、記録したコンテンツを再生又は実行する記録再生装置において、外部記録媒体又はローカルストレージに記録された任意のコンテンツに対してアクセス制限を付加することにより、そのコンテンツによる不正コピーや改ざんを防止できるようにすること、を目的としてなされたものである。

より具体的には、第1に、インストール対象とするコンテンツのインストール処理やロード処理を自動化し、これらの処理を実行する際に実行中のコンテンツは共通した機能（インストール又はロード）を呼び出すことにより、許可されたインストール対象のコンテンツのみをインストール／ロードして不正なコピーを防止すると共に、実行中のコンテンツに対してアクセス制限することにより改ざんを防止できるようにすること、

第2に、コンテンツの信頼度を判定し、その信頼度に応じて、インストール処理やロード処理とは異なるコンテンツ実行時のデータ読み込み処理、書き出し処理に対してアクセ

ス制限を行うことにより、不正なコピー及び改ざんを防止できるようにすること、をその目的とする。

【課題を解決するための手段】

【0006】

第1の技術手段は、AVデータ又はアプリケーションプログラム／データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置において、前記処理手段は、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴としたものである。

【0007】

第2の技術手段は、第1の技術手段において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを有し、前記処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールするインストール処理手段を有することを特徴としたものである。

【0008】

第3の技術手段は、第2の技術手段において、前記インストール処理手段は、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴としたものである。

【0009】

第4の技術手段は、第2又は第3の技術手段において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記特定領域への書き込み処理を実行できないようにしたことを特徴としたものである。

【0010】

第5の技術手段は、第1又は第2の技術手段において、コンテンツの実行領域であるメモリを有し、前記処理手段は、前記記録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードするロード処理手段を有することを特徴としたものである。

【0011】

第6の技術手段は、第5の技術手段において、前記処理手段は、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴としたものである。

【0012】

第7の技術手段は、第1乃至第6のいずれか1の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【0013】

第8の技術手段は、第1乃至第7のいずれか1の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【0014】

第9の技術手段は、第1乃至第8のいずれか1の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

## 【0015】

第10の技術手段は、第1乃至第9のいずれか1の技術手段において、前記記録手段は、コンテンツの再生又は実行に必要なプログラム及びデータを1つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段は、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段は、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴としたものである。

## 【0016】

第11の技術手段は、第1乃至第10のいずれか1の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該再生又は実行中のコンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴としたものである。

## 【0017】

第12の技術手段は、第1乃至第11のいずれか1の技術手段において、前記処理手段は、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴としたものである。

## 【0018】

第13の技術手段は、第12の技術手段において、前記コンテンツの信頼度を、プログラムの記述言語、前記読込手段によって読み込んだコンテンツの読込元となる記録媒体、前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか1又は複数に基づいて設定したことを特徴としたものである。

## 【0019】

第14の技術手段は、A/Vデータ又はアプリケーションプログラム/データを含むコンテンツを読み込む読込手段と、該読み込んだコンテンツを記録する記録手段と、該記録したコンテンツを再生又は実行する処理手段とを有する記録再生装置を用いてコンテンツの構成ファイルへアクセスするためのファイルアクセス方法において、前記記録再生装置によって再生又は実行可能な任意のコンテンツに対して、その処理内容に応じて異なるアクセス制限を付加することを特徴としたものである。

## 【0020】

第15の技術手段は、第14の技術手段において、コンテンツを記録した外部記録媒体を接続するための、あるいはコンテンツを記録したサーバ装置とネットワークを介して接続するための外部インタフェースを前記記録再生装置が備え、前記処理手段が備えるインストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置に記録されているコンテンツを前記記録手段の特定領域にインストールすることを特徴としたものである。

## 【0021】

第16の技術手段は、第15の技術手段において、前記インストール処理手段が、前記外部インタフェースに接続された外部記録媒体又はサーバ装置においてインストールが許可されているコンテンツに対してのみ前記記録手段の特定領域へのインストールを許可することを特徴としたものである。

## 【0022】

第17の技術手段は、第15又は第16の技術手段において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのインストール命令に基づいて前記インストール処理手段にインストール指示し、該インストール処理手段以外によって前記記録手段の特定領域への書き込み処理を実行できないようにしたことを特徴としたものである。

## 【0023】

第18の技術手段は、第14又は第15の技術手段において、コンテンツの実行領域であるメモリを前記記録再生装置が備え、前記処理手段が備えるロード処理手段が、前記記



録手段又は外部記録媒体又はサーバ装置に記録されている実行可能なコンテンツを前記メモリへロードすることを特徴としたものである。

【0024】

第19の技術手段は、第18の技術手段において、前記処理手段が、前記記録再生装置が再生又は実行中のコンテンツからのロード命令に基づいて前記ロード処理手段にロード指示し、該ロード処理手段以外によってロード処理を実行できないようにしたことを特徴としたものである。

【0025】

第20の技術手段は、第14乃至第19のいずれか1の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記メモリにロードされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【0026】

第21の技術手段は、第14乃至第20のいずれか1の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記外部記録媒体に記録された他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【0027】

第22の技術手段は、第14乃至第21のいずれか1の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツが前記記録手段にインストールされた他の又は全てのコンテンツにアクセス出来ないようにすることを特徴としたものである。

【0028】

第23の技術手段は、第14乃至第22のいずれか1の技術手段において、前記記録手段は、コンテンツの再生又は実行に必要なプログラム及びデータを1つのパッケージとしてパッケージ単位で記録して有し、前記ロード処理手段が、前記記録手段に記録されている任意のパッケージを構成する少なくともプログラムの全て又は一部を前記メモリにロードし、前記処理手段が、前記メモリにロードされた前記パッケージを構成するプログラムの全て又は一部を再生又は実行中に、該再生又は実行中のプログラムが該プログラムを含む前記パッケージ以外のパッケージにはアクセスできないようにしたことを特徴としたものである。

【0029】

第24の技術手段は、第14乃至第23のいずれか1の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツの前記記録手段及び外部記録媒体及びサーバ装置及びメモリへのアクセスを全て禁止することを特徴としたものである。

【0030】

第25の技術手段は、第14乃至第24のいずれか1の技術手段において、前記処理手段が、前記記録再生装置が任意のコンテンツを再生又は実行中に、該コンテンツのアクセスを該コンテンツの信頼度に応じて制限することを特徴としたものである。

【0031】

第26の技術手段は、第25の技術手段において、前記コンテンツの信頼度を、プログラムの記述言語、前記読込手段によって読み込んだコンテンツの読込元となる記録媒体、前記読込手段によって読み込んだコンテンツの読込元となるネットワークアドレスのいずれか1又は複数に基づいて設定したことを特徴としたものである。

【発明の効果】

【0032】

本発明によると、AVデータ又はアプリケーションプログラム／データを含むコンテンツを記録した外部記録媒体やサーバ装置にアクセスして該コンテンツをローカルストレージに記録すると共に、記録したコンテンツを再生又は実行する記録再生装置において、外

部記録媒体又はローカルストレージに記録された任意のコンテンツに対してアクセス制限を付加することにより、そのコンテンツによる不正コピー及び改ざんを防止することができる。

これは、第1に、インストール対象とするコンテンツのインストール処理やロード処理を自動化し、これらの処理を実行する際に実行中のコンテンツは各コンテンツに共通した機能（インストール又はロード）を呼び出すことにより、許可されたインストール対象のコンテンツのみをインストール／ロードすることができるため、不正コピーを防止することができる。また、実行中のコンテンツに対してアクセス制限することによって改ざんを防止することができる。

第2に、コンテンツの信頼度を判定し、その信頼度に応じて、インストール処理やロード処理とは異なるコンテンツ実行時のデータ読み込み処理、書き出し処理に対してアクセス制限することにより、不正コピーや改ざんを防止することができる。これは、すなわち、書き出し処理を制限することによって改ざんを防止し、読み込み及び書き出し処理の組み合わせを制限することによって不正なコピーを防止することができる。

【発明を実施するための最良の形態】

#### 【0033】

図1は、本発明の一実施形態に係わる記録再生装置の内部構成例について説明するためのブロック図で、図中、10は記録再生装置で、該記録再生装置10は、処理部11、外部デバイスインタフェース12、デバイスインタフェース13、ネットワークインタフェース14、ユーザインタフェース15から構成される。処理部11は、各インタフェースから得た情報を利用して、AVデータをデコード、もしくはアプリケーションプログラムを実行する。外部デバイスインタフェース12は、外部記録媒体16からAVデータやアプリケーションプログラムなどのデータを読み込み、処理部11に引き渡すことができる。ここで、外部記録媒体16とは、例えば、CD-ROM、CD-R（RW）、DVD-ROMなどを含む光ディスクや、メモリカードなどを指す。この外部記録媒体16に記録されているデータは、記録再生装置10以外で記録されたものであってもよい。

#### 【0034】

以下の説明において、意味のあるまとまりを持ったAVデータもしくはアプリケーションプログラム／データをコンテンツとして定義する。また、AVデータとは映像、音声、もしくはその両方を再生するために必要な情報の全てもしくは一部を指す。また、アプリケーションプログラムとはアプリケーションの実行に必要な情報の全てもしくは一部を指す。上記コンテンツは、例えば、1タイトルに相当するAVデータを構成するファイル全体や、1つのゲーム又はアプリケーションを構成するプログラムファイル及びデータファイル全体から構成されている。

#### 【0035】

ネットワークインタフェース14は、ネットワーク17を介して、ネットワーク17に接続されているサーバ装置（図示せず）からデータをダウンロードし、処理部11に引き渡すことができる。本例では、外部記録媒体16とネットワーク17のいずれからでもデータを取得することが出来る構成としているが、これに限定されず何れか一方だけであっても良い。

#### 【0036】

ユーザインタフェース15は、ディスプレイ18、コントローラ19に接続されている。処理部11は、ユーザインタフェース15を通じてAVデータなどをディスプレイ18に出力してユーザにAVデータを視聴させることができる。また、コントローラ19から入力されるユーザの要求は、ユーザインタフェース15を介して処理部11に伝えられる。

デバイスインタフェース13は、記録媒体（ローカルストレージ）20からデータを読み込んだり、記録媒体20にデータを書き出したりすることができる。ここで、記録媒体20は、内蔵又は外付けのハードディスク装置や、記録可能な光ディスクやメモリカードなどの記録媒体であってもよい。記録媒体20（以下、記録装置20で代表する）に記録

されているデータは、記録再生装置 10 で記録されたデータである。

【0037】

処理部 11 は、予め用意されたコンテンツ（A V データ又はアプリケーションプログラム）もしくはいずれかのインタフェースを経由して読み込んだコンテンツを実行し、その処理のひとつとしてファイルアクセス処理を行う。

【0038】

まず、記録再生装置 10 のファイルアクセス処理には次の 3 種類がある。

（処理 1）コンテンツの全体又は一部を外部記録媒体 16 もしくはネットワーク 17 経由でサーバ装置から読み込み、記録装置 20 に識別可能な形式で記録するインストール処理

（処理 2）コンテンツを再生又は実行するために必要なプログラムやデータを記録装置 20 又は外部記録媒体 16 又はネットワーク 17 経由でサーバ装置から内部メモリ上に読み込むロード処理

（処理 3）コンテンツが自身で生成したデータを書き出す処理及び読み込む処理

【0039】

本発明は、上記ファイルアクセス処理に対して不正なコピー及び改ざんを防止するために以下のようにアクセス制限を付加するものである。

【0040】

まず、上記（処理 1）のコンテンツを外部記録媒体 16 もしくはネットワーク 17 経由でサーバ装置から読み込み、記録装置 20 に識別可能な形式で記録するインストール処理について説明する。

ここで、外部記録媒体 16 もしくはネットワーク 17 経由でアクセス可能なサーバ装置にあるデータのうち、そのデータ提供者が認めたもののみをインストールし、それ以外のデータのインストール、つまり不正なコピーを防止する必要がある。また、インストールしたデータに対して改ざんが行われないようにする必要がある。そこで、インストールに必要な処理を共通化して定義し、実行中のコンテンツは、その共通化した処理にのみトリガを与える。このとき、簡単にインストールを実現するために、意味を持ったひとまとまりのコンテンツ（A V データ又はアプリケーションプログラム）を管理する管理情報がインストール元にあることが望ましい。

【0041】

図 2 は、コンテンツの全体又は一部に対して共通化されたインストール処理の一例を説明するためのフロー図である。まず、記録再生装置 10 は、インストール処理の開始に際し（ステップ S 1）、外部記録媒体 16 もしくはネットワーク 17 経由でアクセス可能なサーバ装置に対してインストールしたいコンテンツの全体又は一部を指定する（ステップ S 2）。そのコンテンツの全体又は一部が、コンテンツ提供者がインストールを許可しているコンテンツであるかどうかを確認する（ステップ S 3）。ここで、具体的な確認方法として、例えば、上記コンテンツの全体又は一部のフォーマットやメタデータなどから判断するようにしてもよい。

【0042】

上記ステップ S 3 において、インストールを許可されたコンテンツの全体又は一部でない場合（N O の場合）エラーを返して終了する（ステップ S 4）。また、上記ステップ S 3 において、インストールを許可されたコンテンツの全体又は一部であった場合（Y E S の場合）、記録装置 20 を確認する。これは、記録装置 20 に十分な空き容量があり、また、すでに記録されているコンテンツの全体又は一部と不整合を起こす可能性が無いかどうかを確認する（ステップ S 5）。

上記ステップ S 5 において、記録装置 20 の容量が足りない、もしくは、すでに記録されているコンテンツの全体又は一部と不整合を起こす可能性がある場合（N O の場合）、エラーを返して終了する（ステップ S 6）。また、上記ステップ S 5 において、記録装置 20 に記録可能である場合（Y E S の場合）、インストールするコンテンツの全体又は一部を特定の管理情報と共に記録装置 20 に記録し（ステップ S 7）、処理成功を返して終了する（ステップ S 8）。ここで、特定の管理情報とは、記録装置 20 上で、インストー

ル済みのコンテンツの全体又は一部を区別して管理するための情報で、コンテンツの全体又は一部の整合性のための情報にもなり、コンテンツの全体又は一部の削除（アンインストール）を行う際にも利用する情報である。

#### 【0043】

図3は、コンテンツの全体又は一部に対して共通化された削除（アンインストール）処理の一例を説明するためのフロー図である。まず、記録再生装置10は、アンインストール処理の開始に際し（ステップS11）、記録装置20上のアンインストールしたいコンテンツの全体又は一部を指定する（ステップS12）。次に、そのコンテンツの全体又は一部が記録装置20にあるかどうかを確かめる（ステップS13）。

上記ステップS13において、コンテンツの全体又は一部が記録装置20に無い場合（NOの場合）、エラーを返して終了する（ステップS14）。また、上記ステップS13において、コンテンツの全体又は一部が記録装置20にある場合（YESの場合）、そのコンテンツの全体又は一部と共に記録した特定の管理情報を用いてコンテンツの全体又は一部に含まれる全てのファイルとその管理情報を記録装置20から削除し（ステップS15）、処理成功を返して終了する（ステップS16）。

#### 【0044】

次に、上記（処理2）のコンテンツを再生又は実行するために必要なプログラムやデータを記録装置20又は外部記録媒体16又はネットワーク17経由でサーバ装置から内部メモリ上に読み込むロード処理について説明する。ここで、ロード処理においても、インストール処理と同様に、ロードに必要な処理を共通化して定義し、実行中のコンテンツは、その共通化した処理にのみトリガを与える。

ロード処理において、記録装置20、外部記録媒体16、もしくはネットワーク17経由でアクセス可能なサーバ装置のいずれからも同様に、コンテンツを再生又は実行するために内部メモリ上にプログラムやデータをロードする。このロード処理は、読み込み処理のみで、書き出し処理を必要としないので、直接、改ざんや不正コピーが行われることはない。

#### 【0045】

次に、（処理3）のコンテンツ自身で生成したデータを書き出す処理及び読み込む処理について説明する。

コンテンツに提供されるファイルシステムは、基本的に記録装置20、外部記録媒体16、もしくはネットワーク17経由でアクセス可能なサーバ装置のいずれにも同様にアクセスすることができる。ただし、読み込み専用の記録媒体に書き出すことは出来ない。例えば、外部記録媒体16がCD-ROMのような読み込み専用の記録媒体であった場合、上記ファイルシステムを用いて外部記録媒体16に書き出すことは出来ない。ここで、上記ファイルシステムには、次の条件が付加される。

・上記（処理2）によって処理部11の内部メモリにロードされたコンテンツ（AVデータ及びアプリケーションプログラム）にはアクセスできない。

これによって、コンテンツが、ロードされたデータを読み込んだり、変更を加えることを禁止することができる。

#### 【0046】

また、上記コンテンツのファイルシステムが、外部記録媒体16に記録された他の又は全てのコンテンツにアクセスできないようにしてもよく、また、記録装置20にインストールされた他の又は全てのコンテンツにアクセスできないようにしてもよい。また、上記ファイルシステムの記録装置20又は外部記録媒体16又はネットワーク17経由したサーバ装置へのアクセス全てを禁止するようにしてもよい。

#### 【0047】

ただし、上記コンテンツは、（処理1）を呼び出すインストール命令及びアンインストール命令、もしくは（処理2）のロード処理を含む再生命令及びアプリケーション実行命令を発行することは可能である。

#### 【0048】

これまでの処理を図4にまとめる。

図4は、図1に示した処理部11の詳細構成例を説明するためのブロック図で、処理部11は、アプリケーション実行部11a、インストール処理部11b、ロード処理部11c及びメモリ11dを含むものとする。記録媒体20<sub>1</sub>、20<sub>2</sub>は、図1に示した記録装置20に含まれる異なる記録部分としてもよく、また、独立した記録媒体であってもよい。また、処理部11は、外部記録媒体16もしくはネットワーク17に接続されたサーバ装置（以下、外部記録媒体16で代表する）にアクセス可能とする。尚、本実施形態では、図1に示した各インタフェースは省略されている。

#### 【0049】

図4において、アプリケーション実行部11aで実行されるアプリケーションは、基本的に記録媒体20<sub>1</sub>、20<sub>2</sub>、外部記録媒体16に記録されているコンテンツ（AVデータもしくはアプリケーションプログラム）にアクセス可能とし、外部記録媒体16への記録も可能である。また、上記アプリケーションはインストール処理部11b及びロード処理部11cに命令を発行することが出来る。

#### 【0050】

インストール処理部11bは、外部記録媒体16に記録されているコンテンツを読み込み、記録媒体20<sub>2</sub>に書き出すことが出来る。また、記録媒体20<sub>2</sub>に記録されているコンテンツを削除することが出来る。このインストール処理部11bは、コンテンツからのインストール命令を受け付けて、インストール処理を実行する。従って、インストール処理時に、コンテンツは外部記録媒体16、記録媒体20<sub>2</sub>に直接アクセスすることはできない。

#### 【0051】

ロード処理部11cは、外部記録媒体16もしくは記録媒体20<sub>2</sub>からコンテンツを読み込み、メモリ11dに書き出すことが出来る。このロード処理部11cは、コンテンツからのロード命令を受け付けて、ロード処理を実行する。従って、ロード処理時に、コンテンツは外部記録媒体16、記録媒体20<sub>2</sub>に直接アクセスすることはできない。

#### 【0052】

メモリ11dは、ロード処理部11cによって書き出されたコンテンツのみを記憶する。これらはアプリケーション実行部11aで実行されるアプリケーション自身であり、アプリケーションが使用する変数などはこの領域には記憶しない。また、このアプリケーションがメモリ11dに記憶されたデータを参照することは出来ない。

#### 【0053】

アプリケーション実行部11aで実行されるアプリケーションプログラム（又はAVデータ、以下、アプリケーションプログラムで代表する）によっては外部記録媒体16に記録されているデータを、記録媒体20<sub>1</sub>、20<sub>2</sub>や、他の外部記録媒体などにコピーすることが出来る。ここで、外部記録媒体16に記録されているデータの作者もしくは提供者が、そのデータのコピーを望んでおらず、その正当性を認めていない場合がある。このように不正なコピーを行うアプリケーションプログラムが存在する可能性を考慮し、アプリケーションプログラムの信頼性を評価し、それに応じて、アクセスを制限する方法について説明する。

#### 【0054】

図5は、アプリケーションプログラムの信頼性に応じたアクセス制限の一例を示した図である。例えば、最も信頼できるアプリケーションプログラムであれば、アプリケーション実行部11aに許可された全てのアクセスを可能とする。やや信頼できるアプリケーションプログラムであれば、外部記録媒体16及び記録媒体20<sub>2</sub>への書き出しのみを禁止する。次に信頼できるアプリケーションプログラムであれば、外部記録媒体16及び記録媒体20<sub>2</sub>からの読み込みのみを許可する。あまり信頼できないアプリケーションプログラムであれば、外部記録媒体16及び記録媒体20<sub>2</sub>へのアクセスを禁止する。ほとんど信頼できないアプリケーションであれば、全てのアクセスを禁止する。ただし、アプリケーションプログラムの信頼性とアクセス制限の組み合わせは上記例に限定されるものでは

ない。また、外部記録媒体 16 及び記録媒体 20<sub>2</sub> を同一に扱うように制限されるものではない。

#### 【0055】

また、アプリケーションプログラムの信頼性の評価方法について以下に例を示す。

例えば、アプリケーションプログラムのメタデータを照合するなどの認証処理によって判断する方法がある。また、複数のアプリケーションプラットフォームを持っている場合、アプリケーションプログラムがいずれのプラットフォーム上で動作するかによってその信頼性を判断する方法がある。例えば、AVデータに含まれるマクロ言語の実行環境は、あまり高度なプログラムを組むことは出来ない。そのため、不正な処理を実現することが出来ないという理由で、信頼性が高いと判断することも出来る。

#### 【0056】

さらに、外部記録媒体 16 が特定のメーカーにしか製造できない読み込み専用の記録媒体であったとする。その場合、外部記録媒体 16 からロードされるアプリケーションプログラムは信頼性が高いと判断するようにしてもよい。同様に、記録装置 20 にインストールされたアプリケーションプログラムのインストール元が、特定のメーカーにしか製造できない読み込み専用の記録媒体であった場合、そのアプリケーションプログラムは信頼性が高いと判断するようにしてもよい。さらに、ネットワーク上のサーバ装置のうち、特定のメーカーにしか製造できない読み込み専用の記録媒体にそのアドレスが信頼に足ると記録されていれば、そのアプリケーションプログラムは信頼性が高いと判断するようにしてもよい。このような条件を組み合わせることによって、アプリケーションプログラムの信頼性を評価することが出来る。

#### 【0057】

次に、これまで説明した記録再生装置 10 について具体的な例を挙げて説明する。

対象となる記録再生装置 10 は、DVD プレーヤのように ROM ディスクに記録された AV データを再生する機能を有している。また、AV データの他に Java (R) 言語で書かれたアプリケーションプログラムを ROM ディスクから読み込んでアプリケーションを実行することが出来る。ROM ディスクに加えてネットワークインタフェースを通じて、AV データやアプリケーションプログラムを実行することも出来る。さらに、記録可能媒体へのインタフェースを持ち、上記 AV データやアプリケーションプログラムをインストールし、上記記録可能媒体から読み込んで再生・実行することが出来る。また、アプリケーションプログラムが任意のデータを上記記録可能媒体に書き出し、読み込むことが出来る。

#### 【0058】

ここで、本実施形態では、AV データとアプリケーションプログラムの双方を再生・実行可能な記録再生装置 10 を例に挙げているが、アプリケーションプログラムのみ実行可能な機器であっても良い。また、本例のアプリケーションプログラムの記述言語は Java (R) 言語に限定されず、例えば BASIC 言語、C 言語、また用意されたマクロ言語などプログラムデータを読み込んで実行可能な環境であればいずれの言語でも良い。また、本例では、AV データやアプリケーションプログラムを読み込むインタフェースとして ROM ディスクとネットワーク双方のインタフェースを用意したが、何れか一方だけでも良い。

#### 【0059】

DVD などの ROM ディスクに記録されたコンテンツは、オーサもしくはプロバイダの意図によって、複製や改造が認められていないものが多い。これらを含む同様の許可されていない複製や改造に対して、本発明の記録再生装置 10 を用いて、コンテンツの複製や改造を防止するための方法について説明する。

#### 【0060】

まず、装置構成について前述した図 1 に基づいて説明する。記録再生装置 10 において、外部記録媒体 16 は ROM ディスク 16、記録装置 20 はハードディスク 20、外部デバイスインタフェース 12 は ROM ディスクインタフェース 12、デバイスインターフェー

ス13はハードディスクインタフェース13として読み替えるものとする。

【0061】

処理部11は各インタフェースから得た情報を利用して、AVデータをデコード、もしくはアプリケーションプログラムを実行する。ROMディスクインタフェース12は、ROMディスク16からAVデータやアプリケーションプログラムなどのデータを読み込み、処理部11に引き渡すことが出来る。ネットワークインタフェース14は、ネットワーク17を介してサーバ装置（図示せず）からデータをダウンロードし、処理部11に引き渡すことが出来る。

【0062】

ユーザインタフェース15は、ディスプレイ18、コントローラ19に接続されている。処理部11は、ユーザインタフェース15からAVデータをディスプレイ18に出力し、ユーザにAVデータを視聴させることが出来る。また、コントローラ19から入力されたユーザの要求は、ユーザインタフェース15を介して処理部11に伝えられる。ハードディスクインタフェース13は、ハードディスク20からデータを読み込んだり、ハードディスク20にデータを書き出したりすることが出来る。ただし、本例のハードディスク20に限定されず、RAMディスクやメモリカードなどでも良い。また、ハードディスク20は記録再生装置10に内蔵あるいは外付けのいずれの形態としても良い。

【0063】

処理部11は、予め用意されたコンテンツ（AVデータ又はアプリケーションプログラム）、もしくは、いずれかのインタフェースを経由して読み込んだコンテンツを実行し、その処理のひとつとしてファイルアクセス処理を行う。

【0064】

まず、ROMディスクインタフェース12もしくはネットワークインタフェース14を介して読み込んだコンテンツ（AVデータ又はアプリケーションプログラム）を、ハードディスクインタフェース13を介してハードディスク20にインストールする処理について説明する。

【0065】

ここでインストールとは、ROMディスク16もしくはネットワーク17を介してアクセス可能なサーバ装置において、ハードディスク20にコピーが認められたコンテンツを、識別可能な形式でハードディスク20に記録することをいう。ここで、インストール可能なひとまとまりのコンテンツをパッケージと呼ぶことにする。例えば、ひとつの映画であり、トレーラー（映画の予告編）であり、また、ゲームである。また、パッケージは、ROMディスク16のコンテンツを補強するものであっても良い。例えば、ROMディスク16のコンテンツには含まれない言語の字幕情報と、それを再生可能にする管理情報などである。

【0066】

ここで、ROMディスク16においてインストールが認められているコンテンツを判別する方法の一例を下記の図6に基づいて説明する。

図6は、ROMディスク16に記録されているファイル構成の一例を示した図である。

図6(A)に示すROMディスク16のファイル構成において、ルートディレクトリ31の下には、videoという名前のフォルダ32と、install.infoという名前のファイル35と、packageという名前のフォルダ36とがある。ここでvideoフォルダ32は、このROMディスク16のAVデータを再生するときに自動的に参照されるフォルダである。このフォルダ32内のindex01.infoという名前のファイル33は再生順序をコントロールする管理情報ファイルであり、content01.mpgという名前のファイル34はAVデータの実体が記録されたファイルである。例えば、index01.infoファイル33がロードされ、その記述に従ってcontent01.mpgファイル34が再生される。ここで、index01.infoファイル33は、再生可能なAVデータを管理しているが、実行可能なプログラムファイルを管理するものであっても良い。もしくは、ファイル33自体が実行可能なプログラム

ファイルであっても良い。また、ひとつの管理情報ファイルが複数のAVデータやプログラムファイルを管理していても良い。さらに、管理情報ファイルが複数であっても良い。その場合、デフォルトでロードされるファイル名が特定される必要がある。`install.info`ファイル35は、インストールが認められているファイルを管理している。

#### 【0067】

図6(B)は、`install.info`ファイル35の内容の一例を示す図である。コピーが認められているファイルへのパスと、管理用かつ表示用のタイトルと、表示用のイメージファイルへのパスが記録されている。`package`フォルダ36には、`index01.info`という名前のファイル37と、`content01.mpg`という名前のファイル38と、`image.jpg`という名前のファイル39とが含まれている。`index01.info`ファイル37は、再生順序をコントロールする管理情報ファイルであり、`content01.mpg`ファイル38はAVデータの実体が記録されたファイルである。

#### 【0068】

図6(B)に示すコピーが認められているファイルは、`index01.info`ファイル37と`content01.mpg`ファイル38であり、表示用のイメージファイルは、`image.jpg`ファイル39であることがわかる。表示用のイメージファイルとは、インストールされたパッケージをユーザに提示する際の代表画像であり、DVDディスクなどのケース表面に印刷されているような画像が考えられる。そして、`install.info`ファイル35に登録されているファイルがインストールの対象となり、登録されていないファイルは、インストールの対象とはならない。また、上記例では、`install.info`ファイル35が管理するのはひとつのパッケージであるが、これに限定されず複数のパッケージを管理しても良い。もしくは、複数のインストール情報ファイルを作成するようにしても良い。

#### 【0069】

図7は、ハードディスク20に記録されているファイル構成の一例を示した図である。ルートディレクトリ41の下に`package.list`という名前のファイル42がある。`package.list`ファイル42は、インストールされた各パッケージを管理する管理情報ファイルであり、また、各パッケージのフォルダをROMディスク16の`video`フォルダと等価に扱うための変換テーブルである。インストールされたパッケージは、システムが用意したフォルダに`video`フォルダと同様の形式で記録される。例えば、`pkg001`フォルダ43に`index01.info`ファイル44と、`content01.mpg`ファイル45のように記録される。これらのデータの再生手段については前述したROMディスクコンテンツの再生手順と同様である。また、表示用のイメージファイルも同じフォルダに記録される。例えば、`image.jpg`ファイル46である。そしてこれらのデータへのパスが、管理用のタイトルと関連付けられて、`package.list`ファイル42に記録されている。

#### 【0070】

また、同様に、`pkg002`フォルダ47には`index01.info`ファイル48と、`content01.mpg`ファイル49のように記録される。表示用のイメージファイルも同じフォルダに記録される。例えば、`image.jpg`ファイル50である。

#### 【0071】

上記の処理はアプリケーションプログラムからインストールコマンドがコールされることによって実行される。インストールコマンドは、例えばデバイスを指定することで、自動的に処理される。デバイスに複数のパッケージが存在するのであれば、管理用のタイトルを取得するコマンドと、管理用のタイトルを指定するインストールコマンドを併用することで実現できる。

#### 【0072】

また、必要であればパッケージのバージョンアップを導入しても良い。同一の管理用タイトルで管理されるパッケージに異なるバージョンが存在する場合に、古いバージョンの



パッケージを新しいバージョンのパッケージに入れ替える処理を自動的に行う。そしてアプリケーションプログラムは、バージョンアップコマンドをコールすることによって実現する。必要に応じて、図6(A)に示したinstall.infoファイル35や、図7に示したpackage.listファイル42にパッケージ及び各ファイルのバージョンを記録する。

#### 【0073】

次に、ROMディスク16、もしくはネットワーク17を介してアクセス可能なサーバ装置、もしくはハードディスク20のコンテンツをロードして、再生・実行する方法について以下に説明する。

コンテンツの再生は、管理情報ファイルを指定することで行われる。この管理情報ファイルの指定方法は2つあり、デバイス上の管理情報ファイルを直接指定する方法と、デバイスにデフォルトで指定されている管理情報ファイルの指定としてデバイスを指定する方法である。ここで、再生・実行ファイルの指定方法について下記の図8に基づいて説明する。

#### 【0074】

図8は、ROMディスク16及びハードディスク20に記録されているファイル構成の他の例を示した図である。

図8(A)に示すROMディスク16のファイル構成において、ルートディレクトリ61以下にはvideoフォルダ62があり、index01.infoファイル63は、content01.mpgファイル64とcontent02.mpgファイル65を、index02.infoファイル66は、content03.mpgファイル67を、others68以下のindex04.infoファイル69は、content04.mpgファイル70をそれぞれ管理している。

#### 【0075】

管理情報ファイルを直接指定する場合、デバイスとしてROMディスク16を指定して、フルパスで管理情報ファイル、例えばindex02.infoファイル66を指定する。また、videoフォルダ62以下のファイルでなくても、例えばindex04.infoファイル69を指定することが出来る。本例の場合、デフォルトで指定されているファイルは、videoフォルダ62以下のindex01.infoファイル63であるので、ROMディスクインタフェース12を指定するとindex01.infoファイル63が再生・実行対象のファイルとして指定されたことになる。

#### 【0076】

また、ネットワーク17を介したサーバ装置に対しても上記と同様の処理が可能である。例えば、サーバ装置の管理情報ファイルを直接指定することが出来る。httpプロトコルであれば、例えば「http://www.sharp.co.jp/index05.info」などと指定することができる。

#### 【0077】

図8(B)に示すハードディスク20のファイル構成において、ハードディスクの扱い方の一例として、ハードディスク20の各パッケージを各管理用タイトルで管理される仮想デバイスとして認識する。ルートディレクトリ71以下、例えば、pkg001フォルダ73とそれ以下のファイル(index01.infoファイル74, content01.mpg75, content02.mpg76, index02.infoファイル77, content03.mpg78, image.jpg79)は、管理用タイトル「AAA」に関連付けられたパッケージ、pkg002フォルダ80とそれ以下のファイル(index01.infoファイル81, content01.mpg82, image.jpg83)は、管理用タイトル「BBB」に関連付けられたパッケージであるとpackage.listファイル72に記録されているものとする。

ここで、管理情報ファイルを直接指定する場合、例えばデバイスとして「AAA」を指定して、フルパスで管理情報ファイルindex02.infoファイル77を指定する。また、デバイス「BBB」のみを指定するとデフォルトに指定されているindex0

1. infoファイル81が指定されたことになる。

【0078】

上記のように指定されたコンテンツは、再生・実行用の特定のメモリに必要なデータをロードすることによって実行される。この処理はアプリケーションプログラムから再生コマンド、もしくは実行コマンドがコールされることによって実行される。

【0079】

次に、任意のアプリケーションプログラムに許可されたアクセスについて説明する。まず、任意のアプリケーションプログラムは、ロードされたメモリ上のコンテンツ（AVデータ又はアプリケーションプログラム）にアクセスすることは出来ない。また、アプリケーションプログラムは、アプリケーションが生成したデータを読み込み、書き込みするための特定の領域をハードディスク20に有している。ここで、特定の領域の例を、下記の図9に基づいて説明する。

【0080】

図9は、ハードディスク20に記録されているファイル構造の他の例を示した図である。ルートディレクトリ91以下、package.list92, pkg001フォルダ93, index01.infoファイル94, content01.mpgファイル95, image.jpgファイル96, pkg002フォルダ97, index01.infoファイル98, content01.mpgファイル99, image.jpgファイル100まではこれまで説明した通りである。本例では、加えてsavedataフォルダ101を有し、savedataフォルダ101以下のファイルをsavedata.listファイル102が管理する。savedata.listファイル102はsavedataフォルダ101以下のファイルを管理する管理ファイルである。savedataフォルダ101以下には、savedata.list（管理情報）ファイル102によって各アプリケーションプログラムに関連付けられた001.datファイル103と002.datファイル104とを有する。任意のアプリケーションプログラムに関連付けられたファイルが特定の領域に相当する。つまり、各アプリケーションプログラムはsavedata.list（管理情報）ファイル102に管理され、savedataフォルダ101以下に用意されたファイルにのみ読み込み、書き出しのアクセスができる。また、各パッケージを形成するフォルダに対してはロード処理と同様のアクセス手順で外部記録媒体16と同じようにアクセスすることができる。

【0081】

さらに、任意のアプリケーションプログラムは、ROMディスク16もしくはネットワーク17を介してアクセス可能なサーバ装置のデータを読み込むことが出来る。

【0082】

これまでのアクセス制限で、少なくとも再生・実行のためにメモリ上にロードされたデータを改ざんすることを禁止することが出来る。しかし、任意のアプリケーションプログラムが、ROMディスク16もしくはハードディスク20もしくはネットワーク17を介してアクセス可能なサーバ装置のデータを読み込み、ハードディスク20に記録することが出来る。これは、記録されたデータの再生もしくは実行の可否に関わらず、認められていないコピーである可能性がある。

【0083】

ここで、アプリケーションプログラムの信頼性に応じて、アクセスの制限を変える方法を適用する。まずアプリケーションの信頼性を判定する方法の例を以下に示す。

例えば、第1に、ROMディスク16が一般のユーザにとって製造困難である場合、特定のメーカによってのみ製造されることになる。つまり、それらのメーカが信頼に足ることがわかれば、ROMディスク16のデータは信頼できる。また、インストールされたデータを改ざんされる恐れが無いことから、ROMディスク16からインストールされたデータも信頼できる。第2に、ROMディスク16に記録されたネットワークアドレスが指し示すサーバ装置のデータ及びそこからインストールされたデータも信頼できる。ただし、ネットワーク自体を偽称することによって問題のある可能性があるのではやや信頼性が

下がる。そして第3に、不特定のネットワークアドレスが指し示すサーバ装置のデータ及びそこからインストールされたデータは最も信頼できないものと判断する。

【0084】

インストールされたデータに関して信頼性の判定基準が必要である場合、package.listファイルなどの管理情報に上記の3つの信頼性レベルを表すフラグを記録しても良い。

【0085】

図10は、3つの信頼性レベルに対して、3つのアクセス制限レベルを適用する一例を示す図である。まず、ROMディスク16への書き出しは、もともと不可能である。最も信頼できる第1の信頼性レベルに相当するアプリケーションプログラムは、不正な処理を行わないと信頼できるとして、ROMディスク16からの読み込み、ハードディスク20のsavedataフォルダ101以下のアプリケーションに対応したファイルへの書き出しと読み込み、ハードディスク20のパッケージ（例えば、pkg001フォルダ93）からの読み込みのアクセスが認められ、ハードディスク20のパッケージ（例えば、pkg001フォルダ93）への書き出しは禁止される。

【0086】

逆に最も信頼できない第3の信頼性レベルに相当するアプリケーションプログラムは、ROMディスク16、ハードディスク20双方へのアクセスを全て禁止される。

そして、やや信頼できる第2の信頼性レベルのアプリケーションプログラムは、以下のいずれかの制限を受ける。ひとつは、ROMディスク16からの読み込み、ハードディスク20のパッケージ（例えば、pkg001フォルダ93）への書き出しと読み込みを禁止する。もうひとつは、ハードディスク20のsavedataフォルダ101以下のアプリケーションに対応したファイルへの書き出しと読み込み、ハードディスク20のパッケージ（例えば、pkg001フォルダ93）への書き出しを禁止する。この何れかを適用することによって、ROMディスク16からハードディスク20へのデータコピーを不可能とする。

【0087】

さらに、外部記録媒体（以下、外部記録媒体A）からロードされたアプリケーションがアクセスできる外部記録媒体を、上記外部記録媒体Aに限定する。また、インストールされたパッケージ（以下、パッケージB）からロードされたアプリケーションがアクセスできるパッケージを、上記パッケージBに限定する。このような機能を実装することで不正コピーの可能性を防止するようにしてもよい。また、アプリケーションからパッケージへの書き込みを禁止することで不正な改ざんを防止するようにしてもよい。

【産業上の利用可能性】

【0088】

本発明の記録再生装置及びファイルアクセス方法は、各種アプリケーションプログラムを実行可能な携帯端末装置や、HDDを内蔵したDVDレコーダなどに好適に利用することができる。

【図面の簡単な説明】

【0089】

【図1】本発明の一実施形態に係わる記録再生装置の内部構成例について説明するためのブロック図である。

【図2】コンテンツの全体又は一部に対して共通化されたインストール処理の一例を説明するためのフロー図である。

【図3】コンテンツの全体又は一部に対して共通化された削除（アンインストール）処理の一例を説明するためのフロー図である。

【図4】図1に示した処理部の詳細構成例を説明するためのブロック図である。

【図5】アプリケーションプログラムの信頼性に応じたアクセス制限の一例を示した図である。

【図6】ROMディスクに記録されているファイル構成の一例を示した図である。

【図 7】ハードディスクに記録されているファイル構成の一例を示した図である。

【図 8】ROMディスク及びハードディスクに記録されているファイル構成の他の例を示した図である。

【図 9】ハードディスクに記録されているファイル構造の他の例を示した図である。

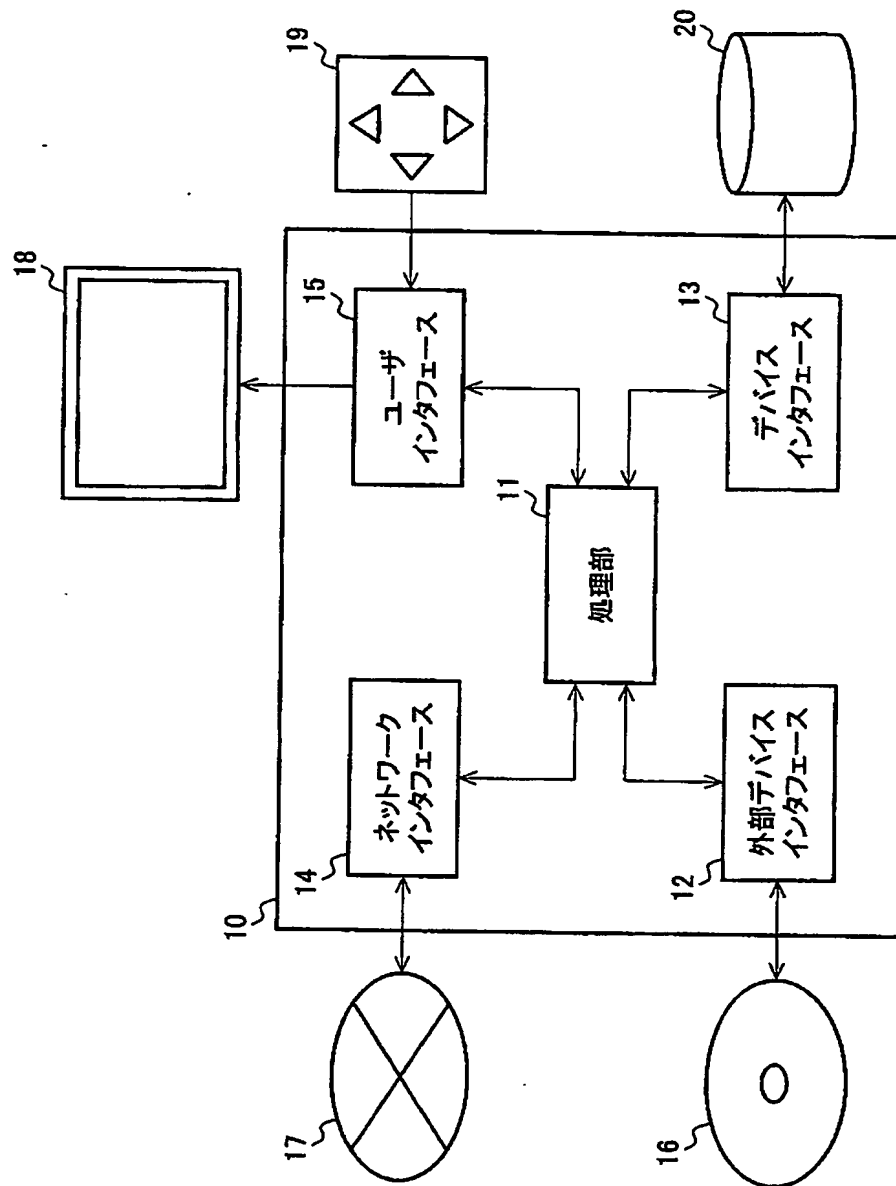
【図 10】3つの信頼性レベルに対して、3つのアクセス制限レベルを適用する一例を示す図である。

【符号の説明】

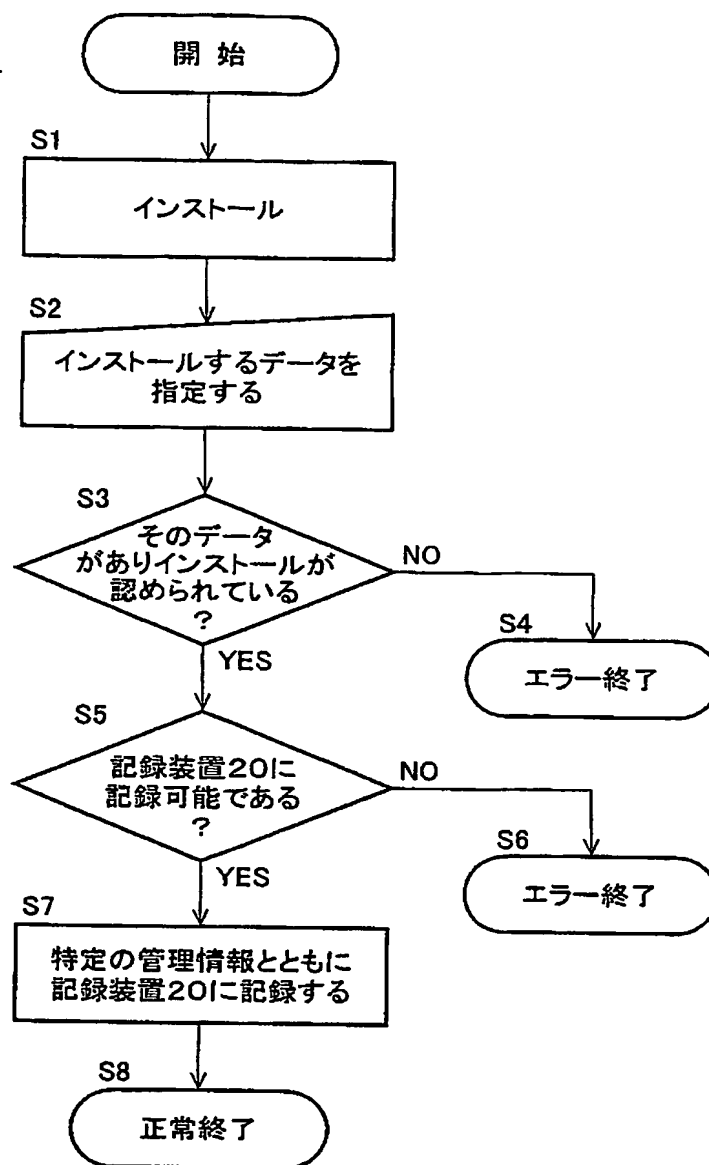
【0090】

10…記録再生装置、11…処理部、11a…アプリケーション実行部、11b…インストール処理部、11c…ロード処理部、11d…メモリ、12…外部デバイスインタフェース、13…デバイスインタフェース、14…ネットワークインタフェース、15…ユーザインタフェース、16…外部記録媒体、17…ネットワーク、18…ディスプレイ、19…コントローラ、20…記録装置（記録媒体）、20<sub>1</sub>、20<sub>2</sub>…記録媒体。

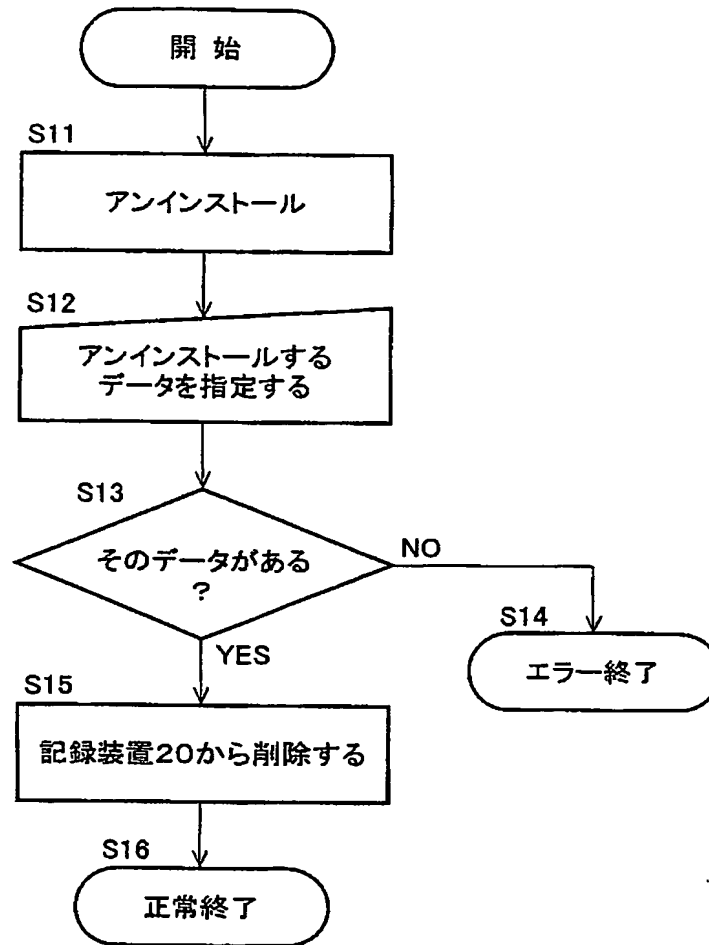
【書類名】 図面  
【図 1】



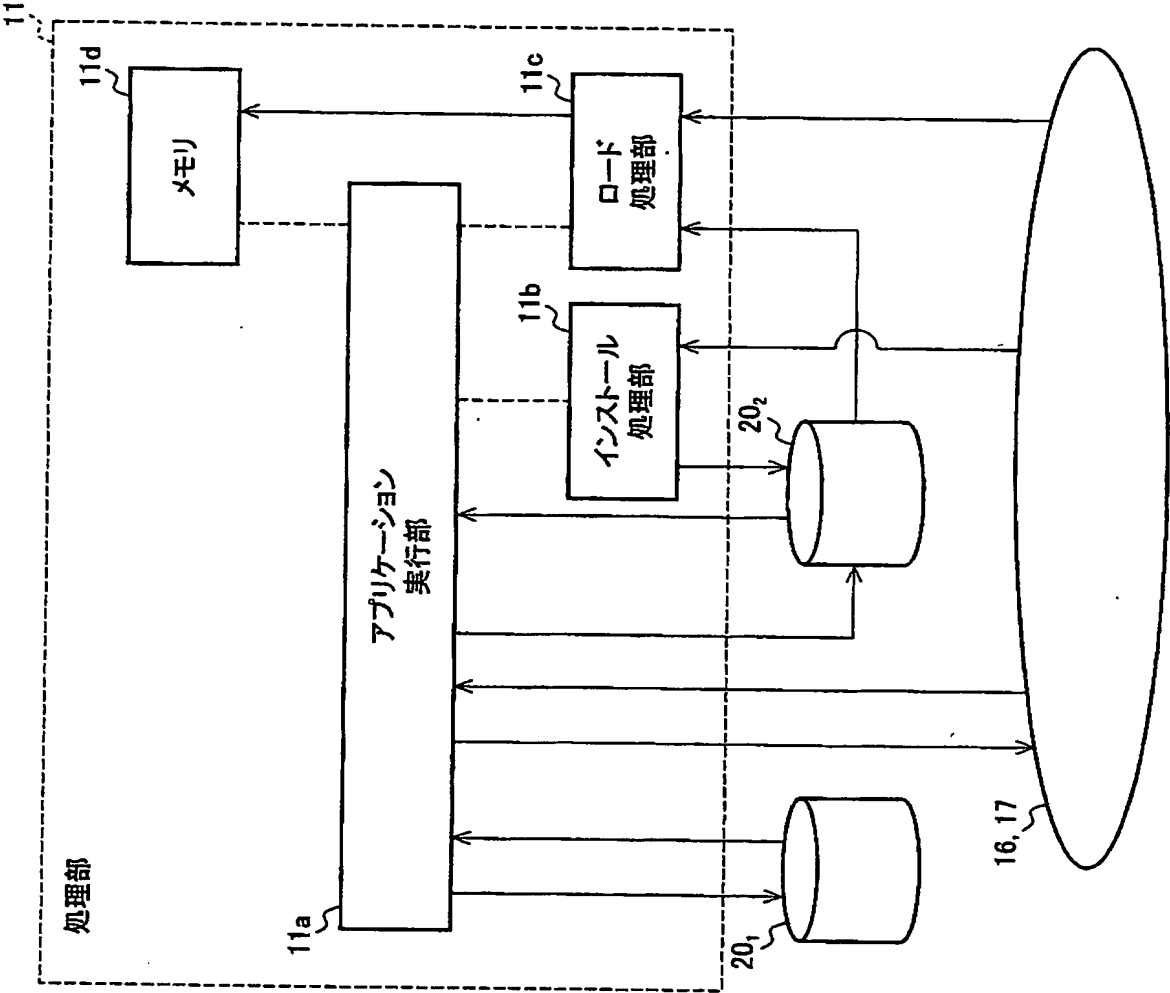
【図 2】



【図 3】



【図 4】

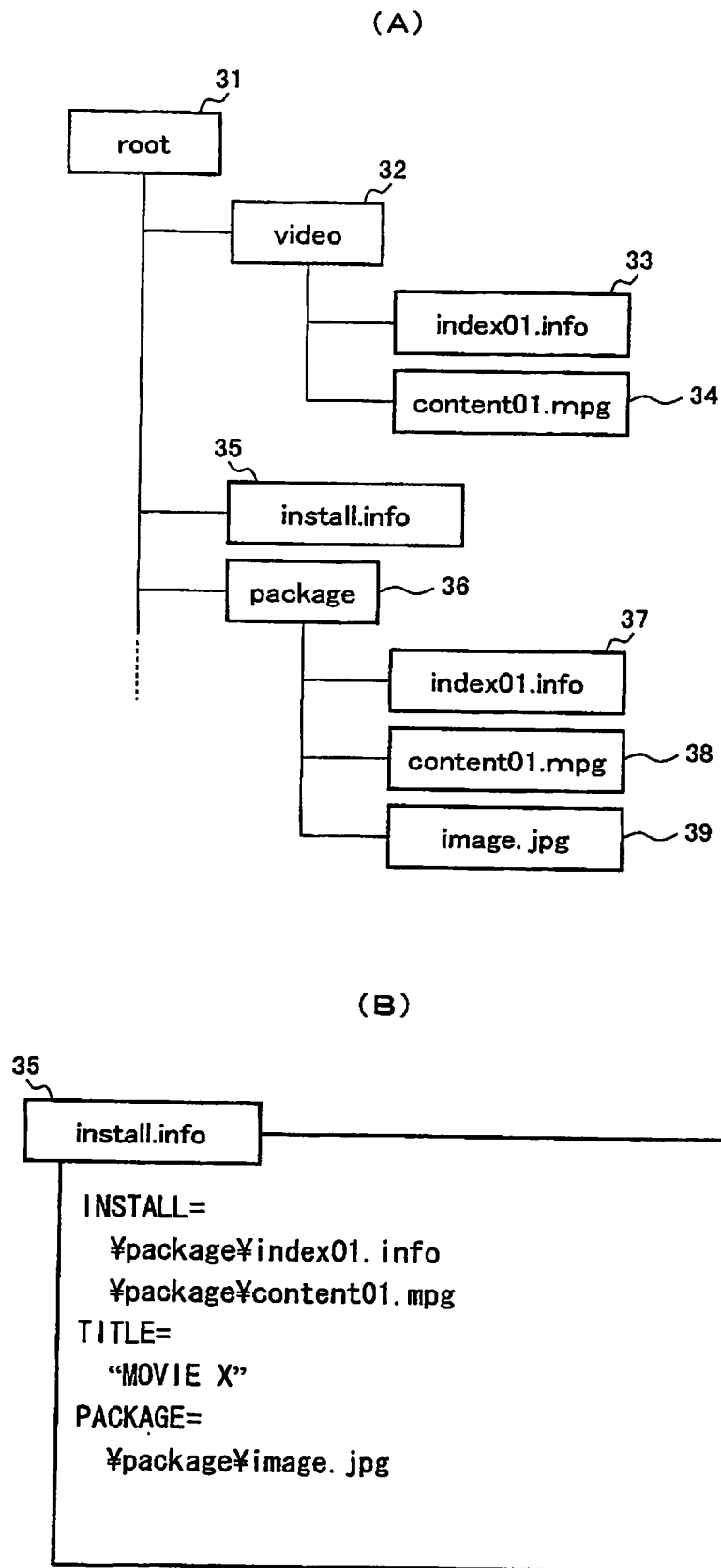




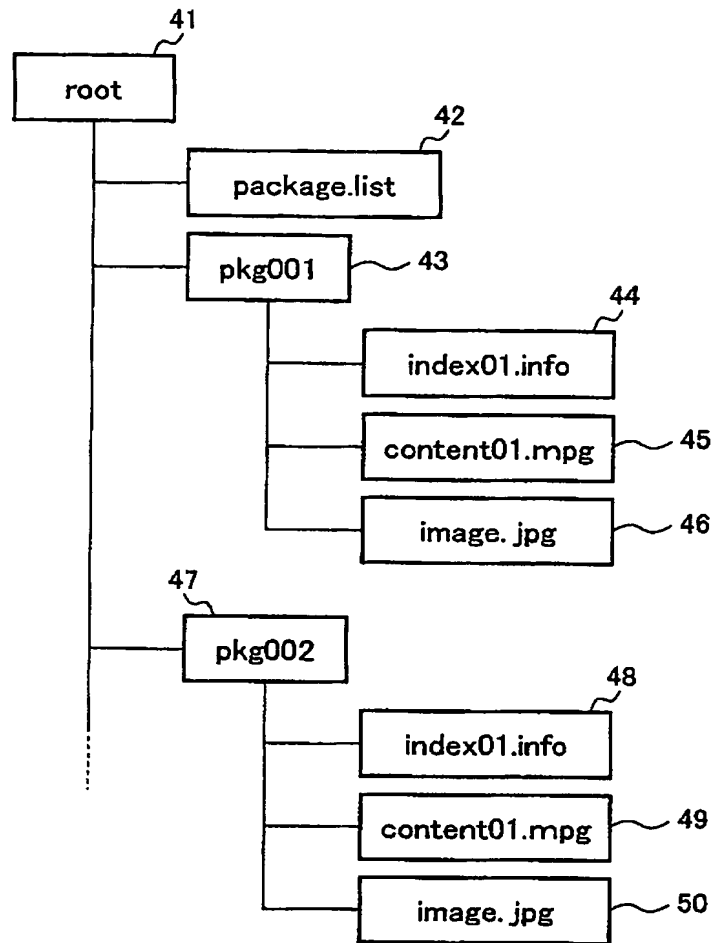
【図 5】

	外部記録媒体16 及び記録媒体20 <sub>2</sub> からの読み込み	外部記録媒体16 及び記録媒体20 <sub>2</sub> への書き出し	記録装置20 からの読み込み	記録装置20 への書き出し
信頼度大	許可	許可	許可	許可
↑	許可	禁止	許可	許可
信頼度中	許可	禁止	禁止	禁止
↓	禁止	禁止	許可	許可
信頼度小	禁止	禁止	禁止	禁止

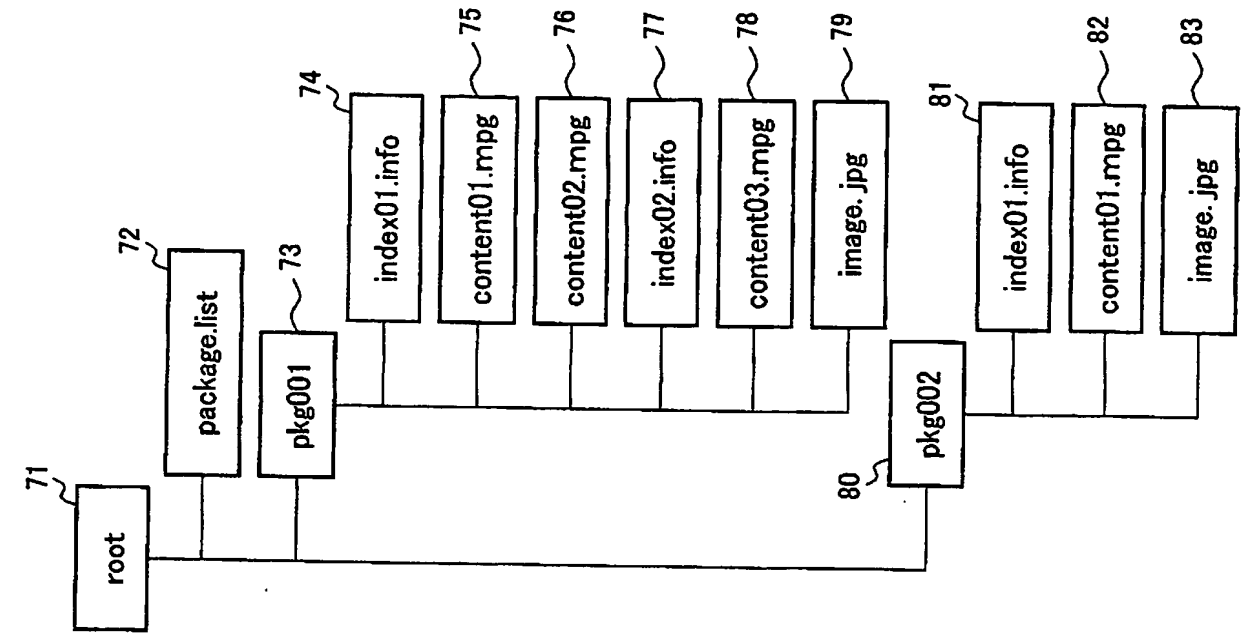
【図 6】



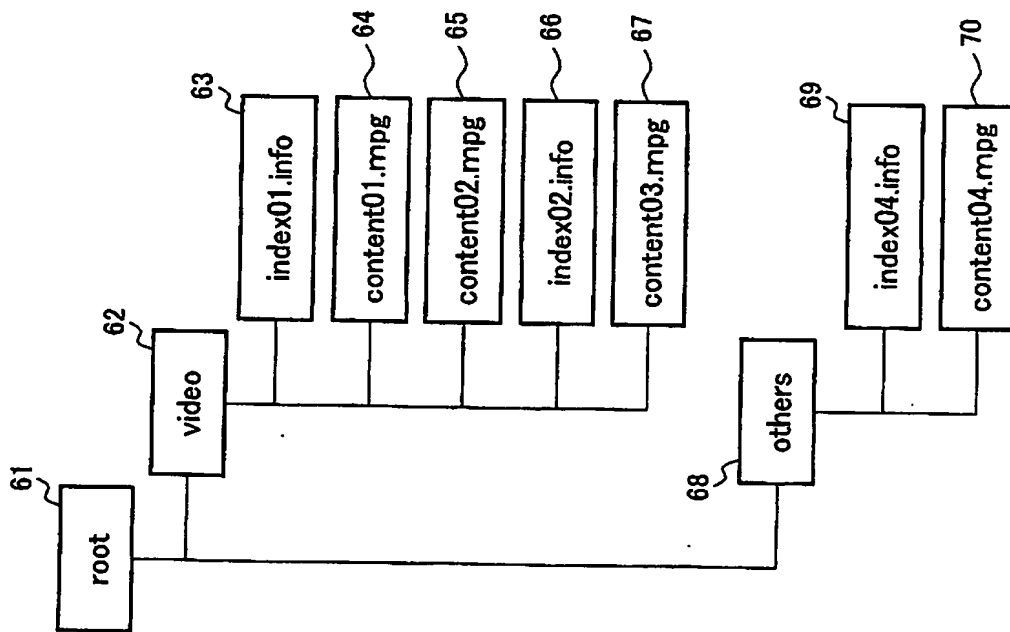
【図 7】



【図 8】

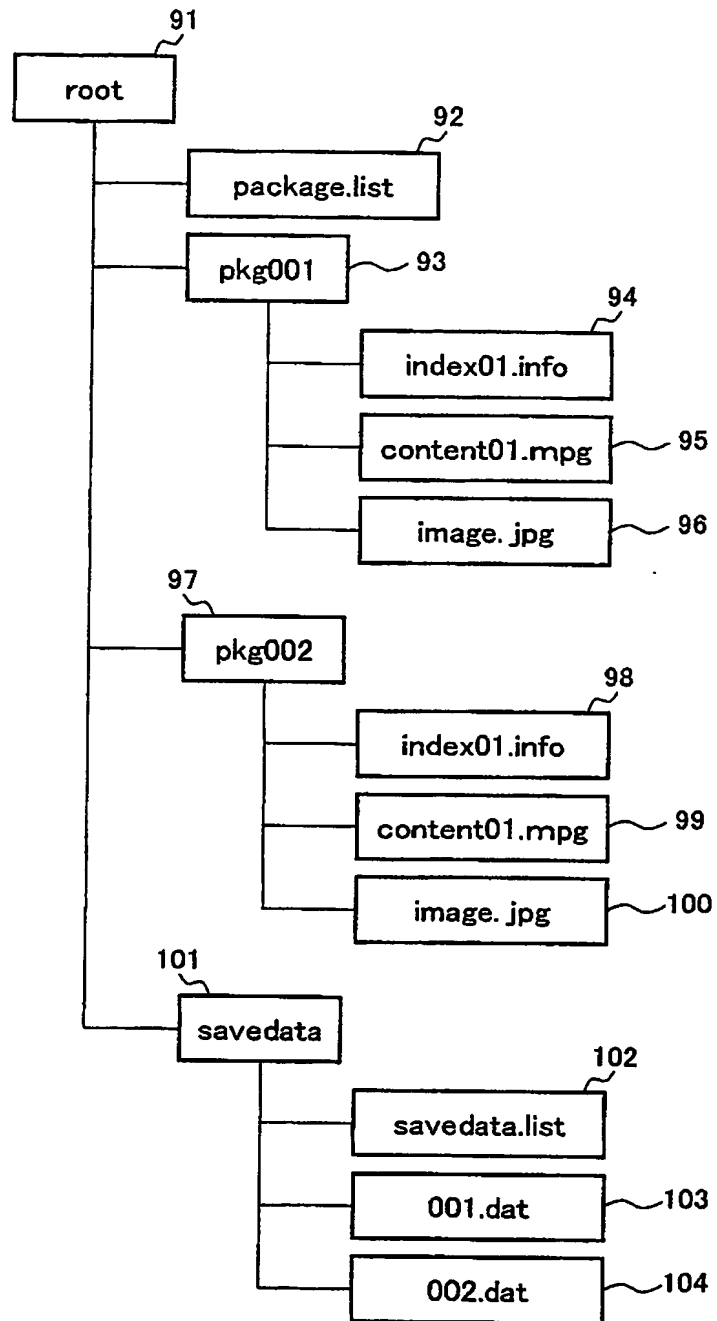


(B)



(A)

【図 9】



【図10】

	ROMディスク16 からの読み込み	ハードディスク20 のsavedata からの読み込み	ハードディスク20 のsavedata への書き出し	ハードディスク20 のパッケージ からの読み込み	ハードディスク20 のパッケージ への書き出し
第1の信頼性レベル (信頼できる)	許可	許可	許可	許可	禁止
第2の信頼性レベル (やや信頼できる)	禁止	許可	許可	禁止	禁止
	許可	禁止	禁止	許可	禁止
第3の信頼性レベル (信頼できない)	禁止	禁止	禁止	禁止	禁止

【書類名】要約書

【要約】

【課題】外部記録媒体等からコンテンツをインストールして再生又は実行する記録再生装置において、任意のコンテンツに対してアクセス制限を付加することで、該コンテンツによる不正コピーや改ざんを防止する。

【解決手段】記録再生装置 10 は、A V データ又はアプリケーションプログラムを含むコンテンツを記録した外部記録媒体 16 を接続する外部デバイス I / F 12 と、外部記録媒体 16 から読み込んだコンテンツを記録する記録装置 20 と、記録したコンテンツを再生又は実行する処理部 11 とを有する。処理部 11 は、記録再生装置 10 によって再生又は実行可能な任意のコンテンツに対して、インストール処理、ロード処理、コンテンツ実行処理に応じて異なるアクセス制限を付加し、コンテンツ実行処理においてはコンテンツのアクセスを該コンテンツの信頼度に応じて制限する。

【選択図】図 1

特願 2 0 0 3 - 3 4 6 2 1 7

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 0 4 9 ]

1. 変更年月日	1 9 9 0 年 8 月 2 9 日
[変更理由]	新規登録
住 所	大阪府大阪市阿倍野区長池町 2 2 番 2 2 号
氏 名	シャープ株式会社



**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☒ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**